

VANGUARD

INTEGRITY PROFESSIONALS

INFORMATION SECURITY EXPERTS

z/OS CA Common Services for RACF STIG

Version: 6

Release: 3

30 June 2023

XSL Release 5/15/2012 Sort by: STIGID
Description:

Group ID (Vulid): V-16932
Group Title: ZB000000
Rule ID: SV-40834r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZCCSR000
Rule Title: CA Common Services installation data sets will be properly protected.

Vulnerability Discussion: CA Common Services installation data sets have the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to these data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

Responsibility: Information Assurance Officer
IACControls: DCSL-1, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Check Content:

a) Consult with your systems programmer to identify the names of the CA Common Services product datasets. (They may begin with SYS2.CCS, SYS2A.CS., or SYS3.CCS).

b) Ensure the following data set controls are in effect for the CA Common Services product data sets:

- UPDATE or higher access to the CA Common Services product data sets is restricted to systems programming personnel.

- UACC (None) and NOWARNING are specified for the CA Common Services product data sets..

- The RACF data set rules for the CA Common Services data sets specify that all accesses of UPDATE or higher (i.e., failures and successes) will be logged.

c) Verify as follows:

1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press ENTER

2. Tab down to Data Set row, type LV next to the dataset profile for the CA Common Services data sets.

3. Check that UACC = None and Warning = No on the dataset profile General Information Screen.

4. Review the Universal Access and Access List on the dataset profile General Information Screen..

5. Repeat steps 1-3 above for any other CA Common Services product dataset profiles.

d) If UPDATE and ALLOCATE (e.g. ALTER) access to the CA Common Services product data sets are restricted to systems programming personnel, there is NO FINDING.

e) If UPDATE and ALLOCATE (ALTER) access to the CA Common Services product data sets is not restricted to systems programming personnel, this is a FINDING.

- f) If UACC = None and Warning = No there is NO FINDING
- g) IF UACC is not None or Warning is not No, this is a FINDING.

Fix Text: The IAO will ensure that WRITE and/or greater access to CA Common Services installation data sets is limited to System Programmers only, and all WRITE and/or greater access is logged. READ access can be given to all authorized users.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have WRITE and/or greater access and if required that all WRITE and/or greater access is logged. He will identify if any additional groups have WRITE and/or greater access for specific data sets, and once documented he will work with the IAO to see that they are properly restricted to the ACP (Access Control Program) active on the system.

Data sets to be protected may begin with:
 SYS2.CCS.
 SYS2A.CCS.
 SYS3.CCS.

The following commands are provided as a sample for implementing data set controls:

```
AD 'sys2.ccs.**' UACC(NONE) OWNER(SYS2) AUDIT(SUCCESS(UPDATE)
FAILURES(READ))
```

```
PE 'sys2.ccs.**' ID(syspautd) ACC(A)
PE 'sys2.ccs.**' ID(authorized users/*) ACC(R)
```

CCI: CCI-000213

CCI: CCI-002234

Group ID (Vulid): V-17452
 Group Title: ZB000030
 Rule ID: SV-40857r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCCSR030

Rule Title: CA Common Services Started Task name will be properly identified and/or defined to the system ACP.

Vulnerability Discussion: CA Common Services requires a started task that will be restricted to certain resources, datasets and other system functions. By defining the started task as a userid to the system ACP, It allows the ACP to control the access and authorized users that require these capabilities. Failure to properly control these capabilities, could compromise of the operating system environment, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: ECCD-1, ECCD-2

Check Content:

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press Enter.
- b) Type 1 for General Resource Profile Summary and Tab down to CLASS: , type STARTED for class name.
- c).Find CAS9 (likely name for the CA- Common Services General Resource profile).
- d). Find the Userid associated with CA Common Services started task under the STDATA segment information of the general resource profile.
- e). Go back to Administrator main menu, select 3;1 (Security Server Reports User Profile) and press ENTER.
- f) Tab down to User ID and enter the User ID found in Step d) above and hit enter.
- g). Page down till the Attributes section of the user profile.
- h) Verify that Protected = Yes.
- i) If Protected = Yes, there is no FINDING.
- j). If Protected = No, there is a FINDING.
- k) If CAS9 is NOT found as a General Resource profile under the STARTED class

in c. above, then check if is defined in the Started Procedures Table (ICHRIN03) as follows:

- 1, From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press ENTER
2. Look for STARTED in the Source column and CAS9 in the Procname column..
3. If the CAS9 started procedure does not have an R in the M column there is
NO FINDING (an R in the M column indicates that either the STARTED TASK USER ID does not have the protected attribute or is not defined (these are both findings)
- 4..If there is an R in the M column, there is a FINDING.

Fix Text: The IAO working with the systems programmer will ensure the CA Common Services Started Task(s) is properly identified and/or defined to the System ACP.

If the product requires a Started Task, verify that it is properly defined to the System ACP with the proper attributes.

Most installation manuals will indicate how a Started Task is identified and any additional attributes that must be specified.

The following commands are provided as a sample for defining Started Task(s):

```
au CAS9 name('STC, CAS9') owner(stc) dfltgrp(stc) nopass
    data('CCS stc')
```

CCI: CCI-000764

Group ID (Vulid): V-17454
 Group Title: ZB000032
 Rule ID: SV-40859r1_rule
 Severity: CAT II
 Rule Version (STIG-ID): ZCCSR032
 Rule Title: CA Common Services Started task will be properly defined to the
 STARTED resource class for RACF.

Vulnerability Discussion: Access to product resources should be restricted to only those individuals responsible for the application connectivity and who have a requirement to access these resources. Improper control of product resources could potentially compromise the operating system, ACP, and customer data.

Responsibility: Information Assurance Officer
IAControls: ECCD-1, ECCD-2

Check Content:

- a) From the Administrator main menu, select 3;4 (Security Server Reports - General Resource Reports) and press ENTER.
- b) Type 1 for General Resource Profile Summary and Tab down to CLASS: , type STARTED for class name.
- c). Find the general resources profile for the CA Common Services started task, usually called CAS9.*.
- d). If CAS9 is found as a General Resource profile under the STARTED class, there is no FINDING. .
- e) If CAS9 is NOT found as a General Resource profile under the STARTED class, check if is defined in the Started Procedures Table (ICHRIN03) as follows:
 - 1, From Analyzer main Menu, go to 3;4 (Online Displays Started Procedures Analysis) and Press ENTER
 - 2. Look for STARTED in the Source column and CAS9 in the Procname column..
 - 3. If CAS9 is not found either as a General Resource Profile under STARTED class in c. above AND not found in the Started Procedures Table (ICHRIN03) either, this is a FINDING.

Fix Text: The IAO working with the systems programmer will ensure the CA Common Services Started Task(s) is properly identified and/or defined to the System ACP.

A unique userid must be assigned for the CA Common Services started task(s) thru a corresponding STARTED class entry.

The following commands are provided as a sample for defining Started Task(s):

```
rdef started CAS9.** uacc(none) owner(admin) audit(all(read))
      stdata(user(CAS9) group(stc))
setr racl(started) ref
```

CCI: CCI-000764

UNCLASSIFIED